

PEMERINTAH
KOTA CIREBON



Standar Operasional Prosedur (SOP) 2024

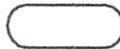
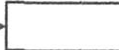
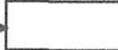
DINAS KOMUNIKASI INFORMATIKA
DAN STATISTIK KOTA CIREBON

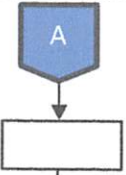
**Bid. Persandian dan
Keamanan Informasi**



 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 59 / 2.2 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2023
	Tanggal Revisi	02 JANUARI 2024
	Tanggal Efektif	02 JANUARI 2023
	Disahkan oleh	 Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : RESET AKUN VPN (VIRTUAL PRIVATE NETWORK)		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Virtual Private Network
Keterkaitan:		Peralatan / Perlengkapan :
Pembuatan akun VPN		1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		Disimpan sebagai data reset akun VPN

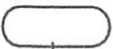
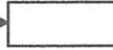
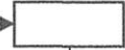
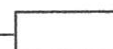
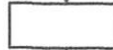
**STANDAR OPERASIONAL PROSEDUR
PERMOHONAN MERESET AKUN VPN**

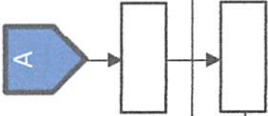
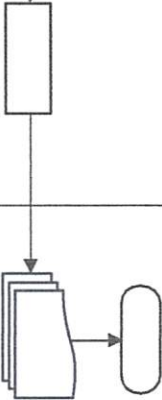
No	Kegiatan	Pelaksana				Waktu	Mutu Baku	Ket
		Perangkat Daerah	Kepala DKIS	Kepala Bidang Persandian dan Keamanan Informasi	Sub Koordinator Layanan Keamanan Informasi		Output	
1	Menyampaikan surat permohonan reset akun VPN					5 menit	Surat permohonan reset akun VPN	
2	Menerima dan menelaah surat permohonan reset akun VPN mendisposisikan kepada Kepala Bidang Persandian dan Kemanan Informasi					10 menit	Surat permohonan reset akun VPN yang sudah di disposisi	
3	Kepala Bidang Persandian dan Keamanan Informasi mendisposisikan ke tim teknis Bidang Persandian					10 menit	Disposisi Kepala Bidang Persandian ke Sub Koordinator Layanan Keamanan Informasi	
4	Sub Koordinator Layanan Keamanan Informasi dan Tim Teknis Bidang Persandian memverifikasi persyaratan pengajuan reset akun VPN dengan catatan: - Jika sesuai, akan direset akun VPN - Jika tidak sesuai, akan ditolak			Ditolak Diterima  	30 Menit	Laporan verifikasi akun VPN		

5	Sub Koordinator Layanan Keamanan Informasi dan Tim Teknis Bidang Persandian mereset akun VPN					30 menit	Mereset akun VPN	
6	Sub Koordinator Layanan Keamanan Informasi melaporkan hasil reset akun VPN kepada kepala DKIS serta membuat surat balasan kepada Perangkat Daerah					15 menit	Laporan hasil reset akun VPN	

 PEMERINTAH KOTA CIREBON	Nomor SOP	DOD.8.3.3/60/1.2.21-SANDI/DKS/2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	
	Tanggal Efektif	02 Januari 2024
	Disahkan oleh	  Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA'RUF NURYASA, AP.MM. NIP. 19780330-199602 1 004
DINAS KOMUNIKASI, INFORMATIKA dan STATISTIK KOTA CIREBON	NAMA SOP : Permohonan Penetration Testing (Pentest)	
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik;		1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. Memiliki kemampuan untuk melakukan Penetration Testing (Pentest) 3. Menguasai SOP Permohonan Penetration Testing (Pentest) 4. Memiliki kemampuan administrasi umum
Keterkaitan:		Peralatan / Perlengkapan :
		1. Komputer
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses penyelenggaraan Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		Disimpan sebagai data Aplikasi yang sudah dilakukan Penetration Testing (Pentest).

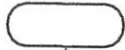
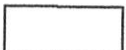
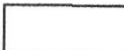
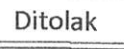
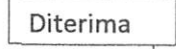
LAMPIRAN : PERMOHONAN PENETRATION TESTING (PENTEST)

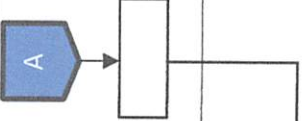
No	Kegiatan	Pelaksana			Mutu Baku		Keterangan
		Pemohon	Kepala DKIS	Bidang Persandian dan Keamanan Informasi	Waktu	Output	
1	Menyampaikan surat pengantar permohonan penetration testing				30 menit	Surat	
2	Menerima surat permohonan penetration testing dari pemohon				60 menit	Surat	
3	Membuat surat pemberitahuan kegiatan Pentest kepada pemohon - Metode Pentest - Waktu Pelaksanaan Pentest - Tim Pelaksana Pentest			 	60 menit	Surat	
4	Melaksanakan Pentest			 	10 HK	Kegiatan	
5	Membuat Laporan Awal Pentest			 	180 menit	Laporan	
6	Membuat Surat Laporan Awal Pentest kepada pemohon			 	60 menit	Surat	
7	Tindak lanjut hasil laporan awal Pentest	  			10 HK	Kegiatan	

8	Evaluasi dan Membuat laporan hasil Penetration Testing			3 HK	Laporan	
8	Membuat Surat Hasil Pentest			60 menit	Surat	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.S.3.3/61/2.21-SANDI/DKIS/2024
	Tanggal Pembuatan	02 JANUARI 2023
	Tanggal Revisi	02 JANUARI 2024
	Tanggal Efektif	02 JANUARI 2023
	Disahkan oleh	  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PEMBUATAN AKUN VPN (VIRTUAL PRIVATE NETWORK)		
Dasar Hukum: 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik 2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; 3. Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik; 4. Peraturan Badan Siber dan Sandi negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah; 5. Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon.		Kualifikasi Pelaksana: 1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Virtual Private Network
Keterkaitan: SOP Reset VPN		Peralatan / Perlengkapan : 1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan: Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Pembuatan Akun VPN pada Pemerintah Daerah Kota Cirebon		PENCATATAN DAN PENDAFTARAN: Disimpan sebagai data Pembuatan Akun VPN

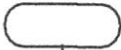
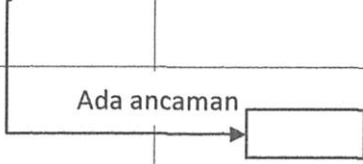
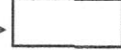
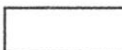
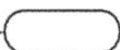
**STANDAR OPERASIONAL PROSEDUR
PERMOHONAN PEMBUATAN AKUN VPN**

No	Kegiatan	Pelaksana				Waktu	Mutu Baku Output	Ket
		Perangkat Daerah	Kepala DKIS	Kepala Bidang Persandian dan Keamanan Informasi	Sub Koordinator Layanan Keamanan Informasi			
1	Menyampaikan surat permohonan pembuatan akun VPN					5 menit	Surat permohonan pembuatan akun VPN	
2	Menerima dan menelaah surat permohonan pembuatan akun VPN mendisposisikan kepada Kepala Bidang Persandian dan Kemanan Informasi					10 menit	Surat permohonan pembuatan akun VPN yang sudah di disposisi	
3	Kepala Bidang Persandian dan Keamanan Informasi mendisposisikan ke tim teknis Bidang Persandian					10 menit	Disposisi Kepala Bidang Persandian ke Sub Koordinator Layanan Keamanan Informasi	
4	Sub Koordinator Layanan Keamanan Informasi dan Tim Teknis Bidang Persandian memverifikasi persyaratan pengajuan pembuatan akun VPN dengan catatan: - Jika sesuai, akan dibuatkan akun VPN - Jika tidak sesuai, akan ditolak				  	30 Menit	Laporan verifikasi akun VPN	

5	Sub Koordinator Layanan Keamanan Informasi dan Tim Teknis Bidang Persandian membuat akun VPN		30 menit	Pembuatan akun VPN	
6	Sub Koordinator Layanan Keamanan Informasi melaporkan hasil pembuatan akun VPN kepada kepala DKIS serta membuat surat balasan kepada Perangkat Daerah		15 menit	Laporan hasil pembuatan akun VPN	

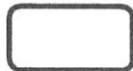
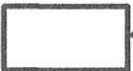
 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 62 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2023
	Tanggal Revisi	02 JANUARI 2024
	Tanggal Efektif	02 JANUARI 2023
	Disahkan oleh	  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : SECURITY OPERATION CENTER (SOC)		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Penanganan Insiden Keamanan Informasi
Keterkaitan:		Peralatan / Perlengkapan :
-		1. Ruang Penanganan Insiden 2. Komputer/Laptop 3. Internet
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP ini tidak dilaksanakan dengan baik maka Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon akan terhambat		Disimpan sebagai data Pengelolaan SOC

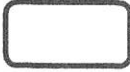
**STANDAR OPERASIONAL PROSEDUR
SECURITY OPERATION CENTER (SOC)**

No	Kegiatan	Pelaksana				Waktu	Mutu Baku Output	Ket
		Tim SOC	Sub koordinator Layanan Keamanan Informasi	Kepala Bidang Persandian dan Keamanan Informasi	Pengelola Jaringan, web site dan aplikasi			
1	- Mengumpulkan, mencatat dan memantau pola lalu lintas jaringan data dari ancaman insiden keamanan - Menganalisis, Mengidentifikasi, potensi ancaman - Perencanaan dan koordinasi tim tanggap insiden					24 jam	Laporan kegiatan pemantauan SOC	
2	Melaporkan ke Kepala Bidang Persandian dan Keamanan Informasi jika terjadi potensi ancaman					1 jam	Menerima laporan dan menganalisa laporan	
3	Menugaskan tim penanganan insiden keamanan informasi untuk melakukan langkah-langkah mitigasi dan pemulihan insiden berdasarkan potensi ancaman					1 jam	Menerima laporan dan menugaskan tim untuk melakukan pemulihan insiden	
4	Melakukan mitigasi dan pemulihan terhadap website dan aplikasi serta berkoordinasi dengan pengelola website dan aplikasi					1 jam	Berkoordinasi dengan pengelola jaringan, web site dan aplikasi	
5	Membuat laporan kegiatan SOC secara keseluruhan baik ada ancaman maupun tidak ada ancaman					30 menit	Laporan kegiatan SOC	

 GEMAH RIPAH LOH JINAWI PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 63 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2023
	Tanggal Revisi	02 JANUARI 2024
	Tanggal Efektif	02 JANUARI 2023
	Disahkan oleh	  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : AKSES MASUK RUANG SERVER		
Dasar Hukum: - Peraturan Presiden (PERPRES) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital; - Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi; - Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik; - Peraturan Wali Kota Cirebon Nomor 61 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik pada Pemerintah Daerah Kota Cirebon.		Kualifikasi Pelaksana: - Kepala Seksi Keamanan Informasi E-Government - Pengelola Ruangan Server
Keterkaitan: -		Peralatan / Perlengkapan : - Identity Card - Rackmount (Rak penyimpanan Server) - Server
Peringatan: Bila server tidak dijaga keamanannya, dikhawatirkan akan terjadi kehilangan/kerusakan yang berdampak pada terganggunya akses pelayanan penyelenggaraan system elektronik pengadaan barang/jasa milik pemerintah		PENCATATAN DAN PENDAFTARAN: - Pihak yang berkepentingan dengan server melaporkan kepetugas sebelum masuk keruangan server - Pencatatan identitas pihak yang ingin mengakses ruang server - Apabila terjadi permasalahan akibat kunjungan tersebut dicatat dibuku tersendiri

**STANDAR OPERASIONAL PROSEDUR
AKSES MASUK RUANG SERVER**

No	Kegiatan				Mutu Baku			Ket
		Petugas Adminitrasi	Koordinator Keamanan Informasi	Kepala Bidang Persandian	Kelengkapan	Waktu	Output	
1	Memastikan pengunjung melakukan pengisian formulir lengkap serta menyerahkan tanda pengenal yang sah				KTP, Perangkat yang dibawa	5 menit	Ada data pengunjung	
2	Koordinator Keamanan Informasi mengecek kelengkapan persyaratan yang diajukan pengunjung				KTP, Perangkat yang dibawa	5 menit	Untuk menjaga keamanan saat berkunjung	
3	Kepala Bidang Persandian memverifikasi formulir dan menentukan apakah ijin akses bisa diberikan atau tidak				Formulir, KTP, dan kelengkapan yang dibawa	5 menit	Jika diberi ijin akses maka akan diberikan tanda pengenal khusus ruangan server untuk dikenakan oleh pengunjung	
4	Koordinator Keamanan Informasi memsadikan selama berada diruangan server pengunjung harus senantiasa ditemani dan diawasi oleh petugas agar pengunjung dipastikan tidak melakukan hal-hal diluar ijin akses atau yang dapat beresiko terhadap server dan isinya			Ya	Tanda pengenal harus senantiasa di kenakan	10 menit	Untuk menjamin keamanan sistem server dan alat-alat yang ada	
5	Petugas adminitrasi memastikan formulir dilengkapi dengan daftar dan nomor seri perangkat yang dibawa (jika ada) dan jam keluar serta mengembalikan tanda pengenal ditukar dengan tanda pengenal diri yang diserahkan	 			Formulir yang dilengkapi dengan daftar dan nomer seri perangkat yang dibawa (jika ada), jam keluar serta	5 menit	Tidak ada masalah dan pengunjung bisa tertib	

	pada awal kunjungan kemudian melaporkan hasil ke koordinator keamanan informasi				tanda pengenal diri			
6	Koordinator Keamanan Informasi melaporkan data hasil pelaksanaan pekerjaan				Data/arsip	5 menit	Kepala Bidang Persandian mengetahui ada berapa pengunjung yang datang	
7	Kepala Bidang Persandian menugaskan petugas administrasi untuk mengarsipkannya				Data/arsip	5 menit	Data arsip bisa aman barangkali mau digunakan	
8	Petugas administrasi mengarsipkan berkas data laporan kunjungan				Data/arsip	5 menit	Arsip dapat tertata dengan baik	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3/64/2.21-SANDI/OKIS/2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	 Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : SOP PENERIMAAN BERITA NASKAH SURAT BIASA MELALUI SUREL SENAPATI		
Dasar Hukum: 1. Perka Lemsaneg No.10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi; 2. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi dan Kabupaten Kota; 3. Peraturan Badan Siber dan Sandi Negara Nomor 19 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah; 4. Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 Tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon.		Kualifikasi Pelaksana: 1. Bertugas di Seksi Persandian Dinas Komunikasi, Informatika dan Statistik Kota Cirebon; 2. Mengetahui dan memahami teknologi informasi dan komunikasi; 3. Mengetahui dan memahami pentingnya pengamanan informasi; 4. Dapat menggunakan email senapati.
Keterkaitan: - SOP Pergelaran Jaring Komunikasi Sandi (JKS)		Peralatan / Perlengkapan : 1. Komputer/Laptop 2. Printer/Scenner 3. Jaringan internet 4. Buku Agenda Surat Masuk 5. Resi 6. Lembar disposisi 7. Cap Stempel
Peringatan: Apabila uraian kegiatan mengalami kendala maka penerimaan Naskah Dinas dari Kementrian/Lembaga Non Kementrian, Pemerintah Provinsi dan Kabupaten/Kota tidak tepat waktu		PENCATATAN DAN PENDAFTARAN: Seluruh dokumen hasil penerimaan disimpan dalam arsip Penerimaan Naskah Dinas Biasa dari Kementria/Lembaga, Non Kementrian, Pemerintah Provinsi dan Kabupaten/Kota

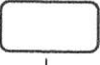
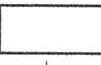
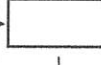
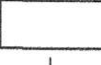
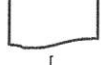
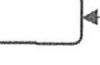
**STANDAR OPERASIONAL PROSEDUR
PENERIMAAN BERITA NASKAH SURAT BIASA MELALUI SUREL SENAPATI**

No	Uraian Prosedure	Pelaksana			SKPD	Mutu Baku			Ket
		Operator Transmisi Sandi	Sub Koor Persandian	Kepala Bidang Persandian dan Keamanan Informasi		Kelengkapan	Waktu	Output	
1	Membuka emai senapati	Mulai				Komputer, Jaringan Internet	10 menit	File surat, Komputer, Jaringan Internet	
2	Meneliti, mengecek, membaca isi, tujuan surat elektronik di email senapati dan apakah perlu diteruskan ke OPD atau Walikota atau Sekda					File surat, Komputer, Jaringan Internet	10 menit	File surat yang telah di teliti	
3	Meneruskan/memforward surat elektronik ke Subkoor Persandian dan Kepala Bidang Persandian dan Keamanan Informasi					File surat yang telah diteliti, Komputer, Jaringan Internet	10 menit	File surat yang telah diteliti,	
4	Meneruskan/memforward surat elektronik ke TU Setda untuk diteruskan ke SKPD sesuai isi surat melalui email @tusetda.cirebonkota.go.id					File, Komputer, Jaringan Internet, email masuk	10 menit	File surat diteruskan ke email TU Setda untuk diteruskan ke SKPD	
5	Mengagendakan dan menyimpan file surat masuk di dalam folder email Senapati	Selesai				Komputer, surat masuk	5 menit	Surat yang telah dibaca dan disimpan	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 65 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	 Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENYELENGGARAAN PELAYANAN PENGACAK SINYAL (JAMMING)		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaga Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846); 2. Peraturan Menteri Komunikasi dan Informatika Nomor 14 Tahun 2016 tentang Pedoman Nomenklatur Perangkat Daerah Bidang Komunikasi dan Informatika; 3. Peraturan Kepala Lembaga Sandi Negara Nomor 19 Tahun 2015 tentang Alat Pendukung Utama Persandian 4. Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 Tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon.		1. Bertugas di Seksi Persandian Dinas Komunikasi, Informatika dan Statistik Kota Cirebon; 2. Memahami dasar sistem jaringan telekomunikasi; 3. Memahami penggunaan alat pengacak sinyal (Jamming); 4. Mampu mengoperasikan alat pengacak sinyal (Jamming); 5. Operator telah mengikuti diklat persandian.
Keterkaitan:		Peralatan / Perlengkapan :
- SOP Penyelenggaraan Pelayanan Siaga Kontra Penginderaan.		1. Peralatan pengacak sinyal (Jamming); 2. Toolkit
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Jika tidak melakukan pemasangan jammer pada acara rapat terbalas, maka ruang rapat tidak steril dari sinyal komunikasi seluler, wifi, radio atau bluetooth		a. Kegiatan pengacak sinyal (Jamming) adalah kegiatan untuk mengacak sinyal pada handphone, wifi, radio atau Bluetooth sehingga sinyal pada alat yang ter-jammer tidak dapat diterima oleh alat lain. b. Kegiatan pengacak sinyal merupakan kegiatan yang dirahasiakan dan diperuntukan pada pengamanan rapat rahasia/terbatas atau kegiatan yang bersifat tertutup lainnya atas permintaan pimpinan OPD.

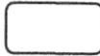
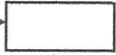
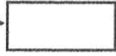
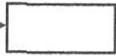


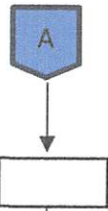
**STANDAR OPERASIONAL PROSEDUR
PENYELENGGARAAN PELAYANAN PENGACAK SINYAL (JAMMING)**

No	Uraian Prosedure	Pelaksana				Mutu Baku			Ket
		Kadis	Kabid	Subkoor	Staf	Kelengkapan	Waktu	Output	
1	Menerima Perintah dari Walikota, Wakil Walikota, Sekda/ Surat Permintaan /permohonan dari SKPD Pemerintah Kota Cirebon					- Lembaran disposisi - Surat - Komputer - Telp/Fax/Email	15 Menit	- Surat Permintaan / disposisi Kepala DKIS	Koordinasi dengan BSSN dan SKPD
2	Menerima disposisi surat dan Kadis mendisposisikan surat ke kabid lalu meneruskan permintaan jamming kepada subkoor persandian					- Lembaran disposisi Kabid - Surat Permohonan	15 Menit	- Surat - Buku agenda - Lembaran Disposisi Kabid	
3	Subkoor menerima disposisi dan membuat surat tugas kepada Tim Operator Jammer					- Lembaran disposisi - Surat - Telp/Email - Computer	15 Menit	- Surat - Personil yang ditunjuk untuk Jamming	
4	Menerima disposisi dan melakukan persiapan peralatan pengacak sinyal (jamming)					- Lembaran disposisi - Surat Permohonan - Peralatan Jammer - Toolkit, Atk	45 Menit	- Menerima surat tugas - Daftar list kelengkapan	
5	Melaksanakan kegiatan dan membuat laporan pelaksanaan kegiatan pengacak sinyal (jamming)					- Lembaran disposisi - Surat Permohonan - Komputer - Telp/Fax/Email	240 menit	- Hasil kegiatan operasional jammer - Kesiapan sarpras waktu disesuaikan	
6	Menerima laporan pelaksanaan kegiatan pengacak sinyal (jamming) untuk selanjutnya diserahkan kepada Kepala Dinas/Badan/Kantor pemohon					- Lembaran disposisi - Surat Permohonan - Laporan pelaksanaan Jamming	30 menit	Arsip dokumen kegiatan	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3/66/2.21-SANDI/DKIS/2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	 Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENYELENGGARAAN PELAYANAN SIAGA KONTRA PENGINDERAAN (COUNTER SURVEILLANCE)		
Dasar Hukum: 1. Kepmendagri Nomor 20 Tahun 2000 tentang Penyelenggaraan Persandian dan Telekomunikasi; 2. Kepmendagri Nomor 34 Tahun 2001 tentang Pengamanan Berita Rahasia Melalui Proses Persandian dan Telekomunikasi; 3. Peraturan Kepala Lembaga Sandi Negara Nomor 19 Tahun 2015 tentang Alat Pendukung Utama Persandian; 4. Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 Tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon.		Kualifikasi Pelaksana: 1. Bertugas di Seksi Persandian Dinas Komunikasi, Informatika dan Memahami konsep dasar sistem operasional TIK; 2. Memahami dasar sistem jaringan telekomunikasi; 3. Memahami sistem administrasi persandian dan keamanan informasi; 4. Memahami penggunaan alat kontra penginderaan; 5. Mampu mengoperasikan alat kontra penginderaan; 6. Bekerja di Unit Teknis Persandian
Keterkaitan: - SOP Penyelenggaraan Pelayanan Pengacak Sinyal		Peralatan / Perlengkapan : 1. Jaring Telepon 2. Jaring data 3. Peralatan Kontra Penginderaan 4. Alat telekomunikasi 5. Meja, Kursi 6. ATK 7. Kendaraan/Mobilitas
Peringatan: 1. Apabila jadwal siaga kontra penginderaan bocor/diketahui oleh pihak yang tidak berkepentingan maka harus dijadwalkan ulang; 2. Pejabat harus ada ditempat dan atau mengizinkan ruang/tempat kerja dan peralatan komunikasi/elektronik bisa dilakukan kontra penginderaan.		PENCATATAN DAN PENDAFTARAN: a. Kegiatan kontra penginderaan adalah kegiatan yang dirahasiakan, maka semua informasi terkait kegiatan ini bersifat rahasia dan tertutup b. Surat menyurat dalam kegiatan kontra penginderaan berklasifikasi dikecualikan (rahasia atau terbatas)

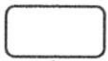
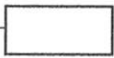
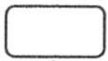
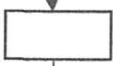
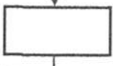
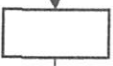
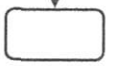
**STANDAR OPERASIONAL PROSEDUR
PENYELENGGARAAN PELAYANAN SIAGA KONTRA PENGINDRAAN (COUNTER SURVEILLANCE)**

No	Uraian Prosedure	Pelaksana				Mutu Baku			Ket
		Kadis	Kabid	Subkoor	Staf	Kelengkapan	Waktu	Ooutput	
1	2	3	4	5	6	7	8	9	10
1	Mengajukan surat permohonan dukungan kerjasama siaga kontra penginderaan kepada Lembaga Sandi Negara. Selanjutnya menerima dan menindaklanjuti disposisi Walikota/Sekda atau surat jawaban Lemsaneg tentang rencana pelaksanaan kontra penginderaan.					- Lembaran disposisi - Surat - Komputer - Telp/Fax/Email	15 Menit	- Surat Permohonan - Surat jawaban	Koordinasi dengan BSSN dan SKPD
2	Kadis mendisposisikan surat ke kabid dan meneruskan kepada subkor persandian					- Lembaran disposisi Kabid - Surat Permohonan	15 Menit	- Surat - Buku agenda - Lembaran Disposisi Kabid	
3	Subkoor melakukan koordinasi dan menyiapkan personil untuk menyusun jadwal dan memetakan lokus yang akan di kontra penginderaan serta membagi tim kerja bersama personil dari BSSN					- Lembaran disposisi - Surat - Telp/Email - komputer	15 Menit	- Surat - Personil / SDM	
4	Membuat dan mengirim surat ijin dan pemberitahuan pelaksanaan siaga kontra penginderaan kepada pejabat dan kepala SKPD dengan skala prioritas dan kerawanan				 	- Lembaran disposisi - Surat Permohonan - Peralatan Jammer - Toolkit - atk	45 Menit	- Surat kepada Pejabat dan SKPD	

5	Melakukan koordinasi dengan tim siaga kontra BSSN dan SKPD yang akan dilakukan siaga kontra penginderaan					- Lembar disposisi - Surat - Computer / laptop - Telp, fax, email	60 menit	Kesiapan sarpras	
6	Pelaksanaan kegiatan dan melaporkan hasil pelaksanaan kegiatan kepada Kepala Dinas Kominfo dan kepada Walikota / Sekda oleh Kabid Persandian dan Keamanan Informasi					- Peralatan kontra penginderaan - Personil/SDM pelaksana kontra penginderaan - Jaringan dan akses data - Transportasi - Computer / laptop - Telp, fax, email	150 menit	Kesiapan /kesediaan pejabat untuk dilakukan kontra penginderaan	Koordinasi dengan BSSN dan SKPD

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 67 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : SOP PENGGELARAN JARING KOMUNIKASI SANDI (JKS)		
Dasar Hukum: 1. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi RI No 35 Tahun 2012 tentang Pedoman Penyusunan SOP Adminitrasi Pemerintahan; 2. Peraturan Pemerintah Dalam Negeri No 52 Tahun 2011 tentang SOP Lingkungan Pemerintahan Provinsi dan Kabupaten/Kota; 3. Keputusan Menteri Dalam Negeri Nomor 34 Tahun 2001 tentang pengamanan berita rahasia melalui proses persandian dan telekomunikasi.		Kualifikasi Pelaksana: 1. Bertugas di Seksi Persandian Dinas Komunikasi, Informatika dan Statistik Kota Cirebon; 2. Memiliki kualifikasi sandi minimal Ahli Sandi Tingkat I; 3. Mengetahui tugas dan fungsi adminitrasi persandian; 4. Operator telah mengikuti diklat persandian.
Keterkaitan: - SOP Penerimaan Berita Naskah Surat Biasa Melalui Surel Sanapati.		Peralatan / Perlengkapan : 1. Komputer, server, laptop 2. Aplikasi berita elektronik 3. Peralatan sandi (aplikasi enkripsi data) 4. Lembar disposisi 5. ATK
Peringatan: Jika SOP ini tidak dijalankan dengan baik, maka proses Penggelaran Jaring Komunikasi Sandi berjalan tidak efektif		PENCATATAN DAN PENDAFTARAN: Kegiatan Jaring Komunikasi Sandi di catat untuk dilaporkan ke pimpinan dan memastikan peralatan sandi terpasang pada jaringan.

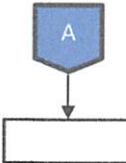
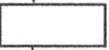
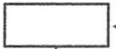
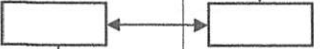
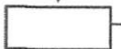
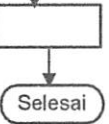
**STANDAR OPERASIONAL PROSEDUR
PENGSELARAN JARING KOMUNIKASI SANDI (JKS)**

No	Uraian Prosedure	Pelaksana			Mutu Baku			Ket
		Operator	Subkoor persandian	Kabid Persandian dan keamanan informasi	Kelengkapan	Waktu	Ooutput	
1	Meminta Kepala Seksi Persandian untuk melakukan gelar Jaring Komunikasi Sandi (JKS)				Memo	10 Menit	Disposisi	
2	Menugaskan sandiman untuk melakukan gelar JKS				Disposisi	10 Menit	Disposisi	
3	Mengecek peralatan sandi, apakah tersedia dan jumlahnya cukup				Disposisi	15 Menit	Data	
4	Melakukan setting system kunci peralatan sandi				Peralatan sandi	15 Menit	Peralatan sandi sudah dipasang sistem kunci	
5	Menghubungkan peralatan sandi dengan jaringan telekomunikasi (jaring telepon, internet atau seluler)				Peralatan sandi yang sudah dipasang system kunci, jaringan telekomunikasi	10 Menit	Peralatan sandi telah terpasang pada jaringan	
6	Mengoprasikan peralatan sandi dalam JKS				Peralatan sandi terpasang pada jaringan	15 Menit	Peralatan sandi siap pakai	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.S 3-3/68/2.21-SANDI/DKS/2024
	Tanggal Pembuatan	02 Januari 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 Januari 2024
	Disahkan oleh	  Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENANGANAN INSIDEN KEAMANAN INFORMASI PADA APLIKASI		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Penanganan Insiden Keamanan Informasi
Keterkaitan:		Peralatan / Perlengkapan :
		1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		Disimpan sebagai data Penanganan Insiden Keamanan Informasi pada Aplikasi

**STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN KEAMANAN INFORMASI PADA APLIKASI**

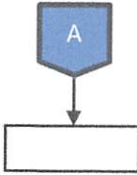
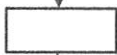
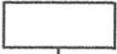
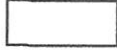
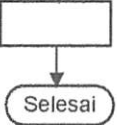
No	Kegiatan	Pelaksana				Mutu Baku		Keterangan
		Pelapor	Bidang Persandian dan Keamanan Informasi	Bidang Layanan E-Government	Ketua CSIRT	Waktu	Output	
1	Menyampaikan laporan/informasi terkait terjadinya insiden keamanan informasi - Jika pelapor eksternal harus membuat surat laporan terjadinya Insiden - Jika Internal tidak	<pre> graph TD Start([Mulai]) --> D1{ } D1 -- Eksternal --> P1[] D1 -- Internal --> P2[] P1 --> D2{ } P2 --> D2 D2 -- Insiden --> P3[] D2 -- Bukan Insiden --> End1([Selesai]) P3 --> A{{A}} </pre>				30 menit	Surat / Laporan	
2	Menerima dan menganalisa laporan/informasi insiden keamanan informasi - Jika termasuk insiden maka dilanjutkan ke proses berikutnya. - Jika bukan insiden maka laporan selesai					60 menit	Laporan	
3	Melakukan Suspend pada Aplikasi terdampak dan melaporkan hasilnya					30 menit	Laporan	

4	Mengirimkan surat pemberitahuan kepada pemilik/pengelola Aplikasi terdampak				120 menit	Surat	
5	Melaporkan surat pemberitahuan Insiden Keamanan Informasi				30 menit	Surat	
6	Melakukan backup Aplikasi terdampak				180 menit	File backup	
7	Melakukan Pemulihan Aplikasi terdampak			3 HK			
8	Membuat Laporan Hasil Penanganan Insiden Keamanan Informasi				60 menit	Laporan	
9	Melaporkan Hasil Penanganan Insiden Keamanan Informasi kepada pemilik/pengelola Aplikasi terdampak				30 menit	Laporan	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.0.3.3 / 70 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  MA'RUF NURYASA, AP.MM. NIP.19760330 199602 1 004
NAMA SOP : PENANGANAN INSIDEN KEAMANAN INFORMASI PADA WEBSITE		
Dasar Hukum: 1. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		Kualifikasi Pelaksana: 1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Penanganan Insiden Keamanan Informasi
Keterkaitan:		Peralatan / Perlengkapan : 1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan: Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		PENCATATAN DAN PENDAFTARAN: Disimpan sebagai data Penanganan Insiden Keamanan Informasi pada website

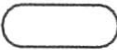
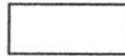
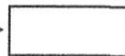
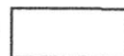
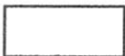
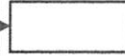
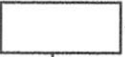
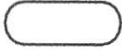
**STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN KEAMANAN INFORMASI PADA WEBSITE**

No	Kegiatan	Pelaksana				Mutu Baku		Keterangan
		Pelapor	Bidang Persandian dan Keamanan Informasi	Bidang Infrastruktur dan TIK	Ketua CSIRT	Waktu	Output	
1	Menyampaikan laporan/informasi terkait terjadinya insiden keamanan informasi - Jika pelapor eksternal harus membuat surat laporan terjadinya Insiden - Jika Internal tidak	<pre> graph TD Start([Mulai]) --> Dec1{ } Dec1 -- Eksternal --> Box1[] Dec1 -- Internal --> Box2[] </pre>				30 menit	Surat / Laporan	
2	Menerima dan menganalisa laporan/informasi insiden keamanan informasi - Jika termasuk insiden maka dilanjutkan ke proses berikutnya. - Jika bukan insiden maka laporan selesai		<pre> graph TD Box1[] --> Box3[] Box2[] --> Box3 Box3 --> Dec2{ } Dec2 -- Insiden --> Box4[] Dec2 -- Bukan Insiden --> End([Selesai]) </pre>			60 menit	Laporan	
3	Melakukan Suspend pada Website terdampak dan melaporkan hasilnya			<pre> graph TD Box4[] --> IconA[A] </pre>		30 menit	Laporan	

4	Mengirimkan surat pemberitahuan kepada pemilik/pengelola Website terdampak				120 menit	Surat	
5	Melaporkan surat pemberitahuan Insiden Keamanan Informasi				30 menit	Surat	
6	Melakukan backup Website terdampak				180 menit	File backup	
7	Melakukan Pemulihan Website terdampak				10 HK		
8	Membuat Laporan Hasil Penanganan Insiden Keamanan Informasi				60 menit	Laporan	
9	Melaporkan Hasil Penanganan Insiden Keamanan Informasi kepada pemilik/pengelola Website terdampak				30 menit	Laporan	

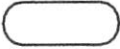
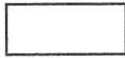
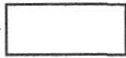
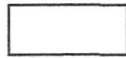
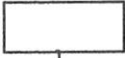
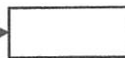
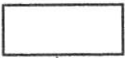
 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3/69/2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PEMBARUAN SERTIFIKAT ELEKTRONIK		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; 3. Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik; 4. Peraturan Badan Siber dan Sandi negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah; 5. Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon.		1. Mampu mengoperasikan komputer dengan baik 2. Memiliki pengetahuan dan keterampilan IT 3. Memiliki kemampuan administrasi umum 4. Menguasai SOP Penerbitan, Pembaharuan dan Pencabutan Sertifikat Elektronik
Keterkaitan:		Peralatan / Perlengkapan :
1. SOP Penertiban Sertifikat Elektronik 2. SOP Pencabutan Sertifikat Elektronik		1. Ruang Rapat 2. Proyektor/LCD 3. Bahan Paparan 4. Laser Pointer 5. PC/Laptop 6. Koneksi Internet
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP tidak dijalankan maka yang terjadi adalah : 1. Tidak tercapainya kepuasan pelanggan 2. Proses pelayanan sertifikat elektronik terhambat		1. Daftar Hadir 2. Notulen

STANDAR OPERASIONAL PROSEDUR PEMBARUAN SETTIFIKAT ELEKTRONIK

NO	Kegiatan	Pelaksanaan					MUTU BAKU			KET
		Pemohon	Subkor Pelayanan Persandian	Kepala Bidang Persandian dan Keamanan Informasi	Kepala Dinas	BSrE	KELENGKAPAN	WAKTIU	OUTPUT	
1	Pemilik sertifikat elektronik melaporkan Kunci privat dan sertifikat elektronik hilang/ rusak /tidak dapat diakses , kepada OP dan sesegera mungkin menyampaikan permohonan pembaruan sertifikat elektronik kembali						Surat permohonan pembaruan sertifikat elektronik dan dokumen penunjang	1 hari	Surat permohonan pembaruan sertifikat elektronik	
2	- Subkoor membuat surat permohonan pembaruan sertifikat elektronik ke BSrE dan pamarafan - Kabid melakukan pengecekan dan pamarafan surat permohonan pembaruan sertifikat elektronik ke BsrE - Kadis melakukan penandatanganan surat permohonan pembaruan sertifikat elektronik						Surat dan dokumen permohonan pengajuan pembaruan sertifikat elektronik	1 hari	Berkas pembaruan sertifikat elektronik	
3	Pengiriman surat permohonan pembaruan sertifikat elektronik						Surat dan dokumen permohonan pembaruan sertifikat elektronik	1 hari	Berkas pembaruan sertifikat elektronik	
4	Proses pembaruan sertifikat elektronik dari BSrE						Surat dan dokumen permohonan pembaruan sertifikat elektronik	1 minggu	Berkas pembaruan sertifikat elektronik	
5	Penerimaan pembaruan sertifikat elektronik dari BsrE						Dokumen pembaruan sertifikat elektronik	1 hari	Pembaruan sertifikat elektronik sudah diterima dari BSrE	
6	Penerimaan pembaruan sertifikat elektronik kepada pemohon						Dokumen pembaruan sertifikat elektronik	1 hari	Pembaruan sertifikat elektronik sudah diterima pemohon	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 71 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENCABUTAN SERTIFIKAT ELEKTRONIK		
Dasar Hukum: 1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		Kualifikasi Pelaksana: 1. Mampu mengoperasikan komputer dengan baik 2. Memiliki pengetahuan dan keterampilan IT 3. Memiliki kemampuan administrasi umum 4. Menguasai SOP Asistensi Penerbitan, Pembaharuan dan Pencabutan Sertifikat Elektronik
Keterkaitan: 1. SOP Penerbitan Sertifikat Elektronik 2. SOP Pembaruan Sertifikat Elektronik		Peralatan / Perlengkapan : 1. Ruang Rapat 2. Proyektor/LCD 3. Bahan Paparan 4. Laser Pointer 5. PC/Laptop 6. Koneksi Internet
Peringatan: Apabila SOP tidak dijalankan maka yang terjadi adalah : 1. Tidak tercapainya kepuasan pelanggan 2. Proses pelayanan sertifikat elektronik terhambat		PENCATATAN DAN PENDAFTARAN: 1. Daftar Hadir 2. Notulen

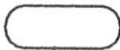
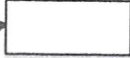
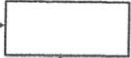
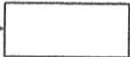
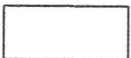
**STANDAR OPERASIONAL PROSEDUR
PENCABUTAN SERTIFIKAT ELEKTRONIK**

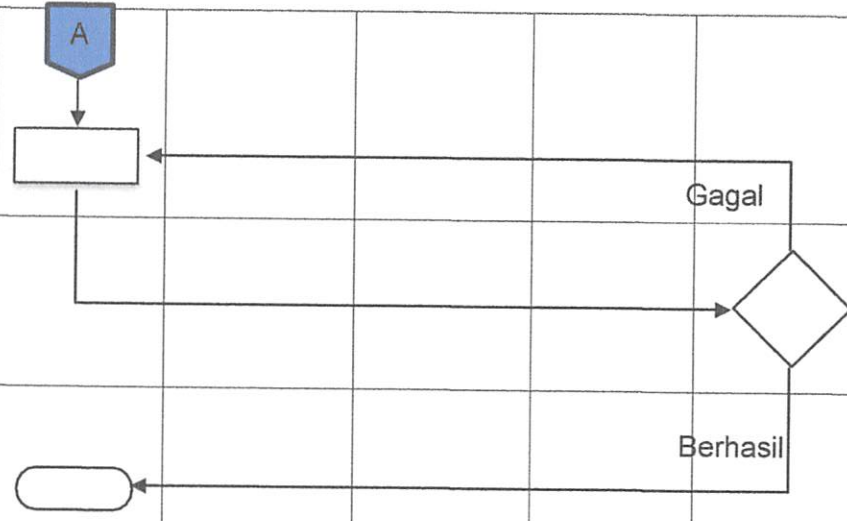
NO	Kegiatan	Pelaksanaan					MUTU BAKU			KET
		Perangkat Daerah	Subkor Pelayanan Persandian	Kepala Bidang Persandian dan Keamanan Informasi	Kepala Dinas	BSrE	KELENGKAPAN	WAKTIU	OUTPUT	
1	Perangkat Daerah melaporkan kepada OP untuk mencabut sertifikat elektronik dikarenakan yang bersangkutan sudah tidak bekerja/pensiun						Surat permohonan pencabutan sertifikat elektronik dan dokumen penunjang	1 hari	Berkas surat permohonan pencabutan sertifikat elektronik	
2	- Subkoor membuat surat permohonan pencabutan sertifikat elektronik ke BSrE dan pamarafan - Kabid melakukan pengecekan dan pamarafan surat permohonan pencabutan sertifikat elektronik ke BSrE - Kadis melakukan penandatanganan surat permohonan pencabutan sertifikat elektronik						Surat dan dokumen permohonan pencabutan sertifikat elektronik	1 hari	Berkas pencabutan sertifikat elektronik	
3	Pengiriman surat permohonan pencabutan sertifikat elektronik						Surat dan dokumen permohonan pencabutan sertifikat elektronik	1 hari	Berkas pencabutan sertifikat elektronik	
4	Proses pencabutan sertifikat elektronik dari BSrE						Surat dan dokumen permohonan pencabutan sertifikat elektronik	1 minggu	Berkas pencabutan sertifikat elektronik	
5	Penerimaan dokumen pencabutan sertifikat elektronik dari BSrE						Dokumen pencabutan sertifikat elektronik	1 hari	Dokumen pencabutan sertifikat elektronik sudah diterima dari BSrE	
6	Penerimaan dokumen pencabutan sertifikat elektronik sesuai dengan ajuan pelapor						Dokumen pencabutan sertifikat elektronik	1 hari	Dokumen pencabutan sertifikat elektronik sudah diterima pelapor	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 72 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  MARUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENERBITAN SERTIFIKAT ELEKTRONIK		
Dasar Hukum: 1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik; 4. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 5. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		Kualifikasi Pelaksana: 1. Mampu mengoperasikan komputer dengan baik 2. Memiliki pengetahuan dan keterampilan IT 3. Memiliki kemampuan administrasi umum 4. Menguasai SOP Asistensi Penerbitan, Pembaharuan dan Pencabutan Sertifikat Elektronik
Keterkaitan: 1. SOP Pencabutan Sertifikat Elektronik 2. SOP Pembaruan Sertifikat Elektronik		Peralatan / Perlengkapan : 1. Ruang Rapat 2. Proyektor/LCD 3. Bahan Paparan 4. Laser Pointer 5. PC/Laptop 6. Koneksi Internet
Peringatan: Apabila SOP tidak dijalankan maka yang terjadi adalah : 1. Tidak tercapainya kepuasan pelanggan 2. Proses pelayanan sertifikat elektronik terhambat		PENCATATAN DAN PENDAFTARAN: 1. Daftar Hadir 2. Notulen



STANDAR OPERASIONAL PROSEDUR
PERMOHONAN DAN PENERBITAN SERTIFIKAT ELEKTRONIK

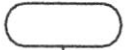
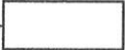
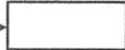
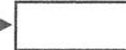
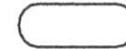
	Kegiatan	Pelaksana					Mutu Baku		Ket
		Pemohon	Kepala DKIS	Ka.Bidang Persandian	Subkor K.I	Verifikator	Waktu	Output	
1	Menyampaikan surat pengantar permohonan penerbitan Sertifikat Elektronik						5 menit	Surat Permohonan Penerbitan Sertifikat Elektronik	
2	Menerima dan menelaah surat permohonan penerbitan sertifikat elektronik dari pemohon dan mendisposisikan ke Kepala Bidang Persandian dan Keamanan Informasi						10 menit	Surat permohonan yang telah disposisi kepada Kepala Bidang Persandian dan Keamanan Informasi	
3	Menerima dan menelaah surat dari Kepala Dinas dan mendisposisikan kepada Subkor Layanan Keamanan Informasi						10 menit	Surat permohonan yang telah disposisi kepada Subkor Layanan Keamanan Informasi	
4	Menerima dan menelaah disposisi surat dari Kepala Bidang dan mendisposisikan kepada verifikator						10 menit	Surat permohonan yang telah disposisi kepada Verifikator	
5	Menerima disposisi dan mendaftarkan penerbitan sertifikat elektronik ke BSR E dan mengisi data nama dan email kedinasan pemohon pada aplikasi AMS					 	5 menit	Pendaftaran pemohon Sertifikat Elektronik pada aplikasi AMS	

6	Melakukan verifikasi / memastikan proses aktivasi berhasil - Jika berhasil, lanjut proses selanjutnya - Jika gagal, verifikasi ulang	 <pre> graph TD A{{A}} --> B[] B --> C{ } C -- Gagal --> B C -- Berhasil --> D([]) </pre>					10 menit	Verifikasi pendaftaran Sertifikat Elektronik	
7	Pengguna menerima email Informasi akun dan tautan set Passphrase, pemohon melakukan set passphrase						5 menit	Akun pengguna pada AMS dan Passphrase	
8	Menunggu persetujuan dan penerbitan Sertifikat Elektronik dari BSR E, Pemohon akan menerima notifikasi pada email bahwa sertifikat elektronik telah diterbitkan						15 menit	Email notifikasi Permohonan Penerbitan Sertifikat Elektronik Berhasil	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3/73/2.21-SANDI/DKIS/2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PERMOHONAN SSL (SECURE SOCKET LAYER) PADA APLIKASI DAN WEBSITE		
Dasar Hukum: 1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon		Kualifikasi Pelaksana: 1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. Memiliki kemampuan mengoperasikan komputer dengan baik 3. Menguasai SOP Permohonan SSL 4. Memiliki kemampuan administrasi umum
Keterkaitan: Penanganan Insiden Keamanan Informasi pada Aplikasi dan Website		Peralatan / Perlengkapan : 1. Komputer
Peringatan: Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses penyelenggaraan Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		PENCATATAN DAN PENDAFTARAN: Disimpan sebagai data Aplikasi/Website yang sudah terpasang SSL (Secure Socket Layer)



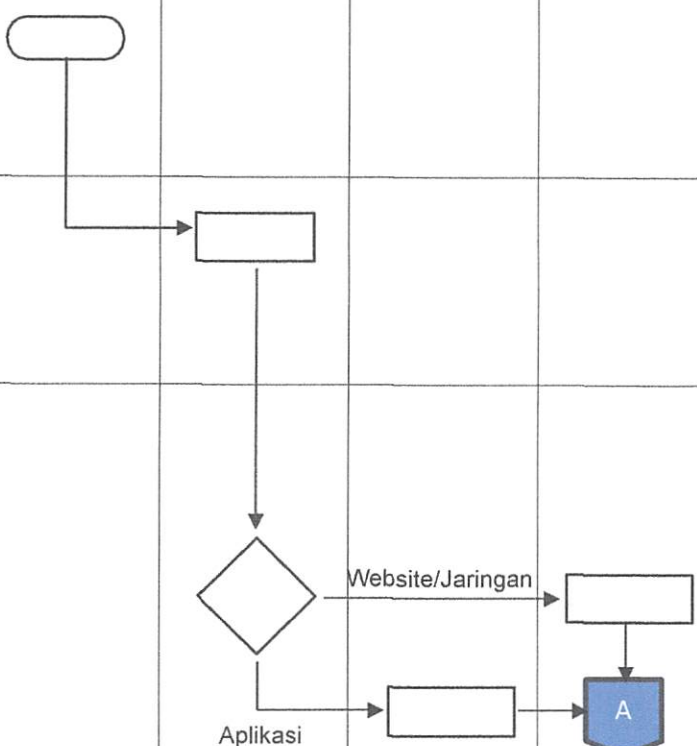
**STANDAR OPERASIONAL PROSEDUR
PERMOHONAN SSL (SECURE SOCKET LAYER) PADA APLIKASI/WEBSITE**

No	Kegiatan	Pelaksana				Mutu Baku		Ket
		Ka.Bidang E-Governmet / Ka. Bidang ITIK	Ka.Bidang Persandian	Subkor Layanan K.I	Staff Layanan KI	Waktu	Output	
1	Menyampaikan Nota Dinas kepada Bidang Persandian dan Keamanan Informasi					5 menit	Nota Dinas	
2	Menerima dan menelaah Nota Dinas dan mendisposisikan ke Subkor Layanan Keamanan Informasi					10 menit	Nota Dinas yang sudah didisposisikan	
3	Menerima dan menelaah disposisi surat dari Kepala Bidang dan mendisposisikan kepada staff					10 menit	Nota Dinas yang sudah didisposisikan	
4	Melakukan Koordinasi : - Jika aplikasi dengan Bidang E-Governent - Jika website dengan Bidang ITIK					20 menit	Laporan	
5	Memberikan Laporan kepada atasan langsung terkait SSL yang sudah terpasang pada Aplikasi/Website					10 menit	Aplikasi/website yang sudah terpasang SSL	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.B.3.3 / 74 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	-
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	  Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon <u>MA'RUF NURYASA, AP.MM.</u> NIP. 19760330 199602 1 004
NAMA SOP : PASCA PENANGANAN INSIDEN KEAMANAN INFORMASI PADA APLIKASI DAN WEBSITE		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon Peraturan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber.		1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Penanganan Insiden Keamanan Informasi
Keterkaitan:		Peralatan / Perlengkapan :
SOP Penanganan Insiden Keamanan Informasi pada aplikasi dan website		1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		Disimpan sebagai data Pasca Penanganan Insiden Keamanan Informasi



STANDAR OPERASIONAL PROSEDUR
PASCA PENANGANAN INSIDEN KEAMANAN INFORMASI PADA APLIKASI DAN WEBSITE

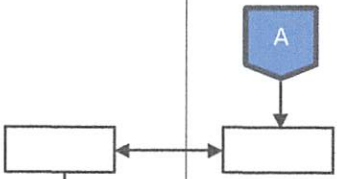
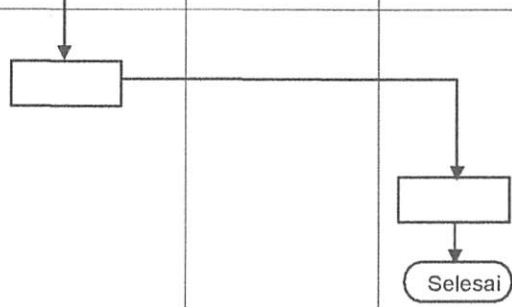
No	Kegiatan	Pelaksana							Mutu Baku	Ket
		Tim Penangan Insiden KI Bidang Persandian	Kepala Bidang Persandian dan Keamanan Informasi	Bidang Layanan E-Gov	Bidang ITIK	Pemilik Aset	Kepala DKIS	Waktu	Output	
1	Menyampaikan surat/laporan/informasi terkait pasca penanganan insiden keamanan informasi pada aplikasi dan atau website							10 menit	Laporan pasca penanganan insiden	
2	Menerima dan menelaah surat/laporan/informasi pasca penanganan insiden keamanan informasi pada aplikasi dan atau website							10 menit	Laporan pasca penanganan insiden yang sudah di disposisi	
3	Kepala Bidang Persandian dan Keamanan Informasi bersama Tim Penangan Insiden Keamanan Informasi menyampaikan laporan pasca penanganan insiden keamanan informasi pada aplikasi dan atau website - Jika Aplikasi kepada Bidang Layanan E-Government - Jika Website kepada Bidang ITIK							10 menit	laporan pasca penanganan insiden keamanan informasi, analisa dan rekomendasi terkait penyebab insiden	

4	Melakukan pengecekan terhadap aset yang terdampak: - Jika Aplikasi, Bidang Layanan E-Government - Jika Website Bidang ITIK	<pre> graph TD A{{A}} --> D{ } D -- "Website/Jaringan" --> R1[] D -- "Aplikasi" --> R2[] R1 --> E1(()) R2 --> E1 </pre>	3 jam	Dokumentasi pasca penanganan insiden	
5	Melaporkan kepada pemilik aset yang terdampak - Jika Aplikasi, Bidang Layanan E-Government - Jika Website Bidang ITIK	<pre> graph TD D{ } -- "Website/Jaringan" --> R1[] D -- "Aplikasi" --> R2[] R1 --> J(()) R2 --> J J --> E1(()) </pre>	10 menit	Laporan pasca penanganan insiden keamanan informasi	
6	Menyampaikan laporan pasca penanganan insiden kepada kepala dinas	<pre> graph TD R[] --> E2(()) </pre>	10 menit	Laporan pasca penanganan insiden keamanan informasi	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	006. 8.3.3 / 103 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 JANUARI 2024
	Tanggal Revisi	
	Tanggal Efektif	02 JANUARI 2024
	Disahkan oleh	 Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon  MASRUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENANGANAN INSIDEN KEAMANAN INFORMASI PADA PUSAT DATA		
Dasar Hukum: 1. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		Kualifikasi Pelaksana: 1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Penanganan Insiden Keamanan Informasi
Keterkaitan:		Peralatan / Perlengkapan : 1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan: Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		PENCATATAN DAN PENDAFTARAN: Disimpan sebagai data Penanganan Insiden Keamanan Informasi pada Pusat Data

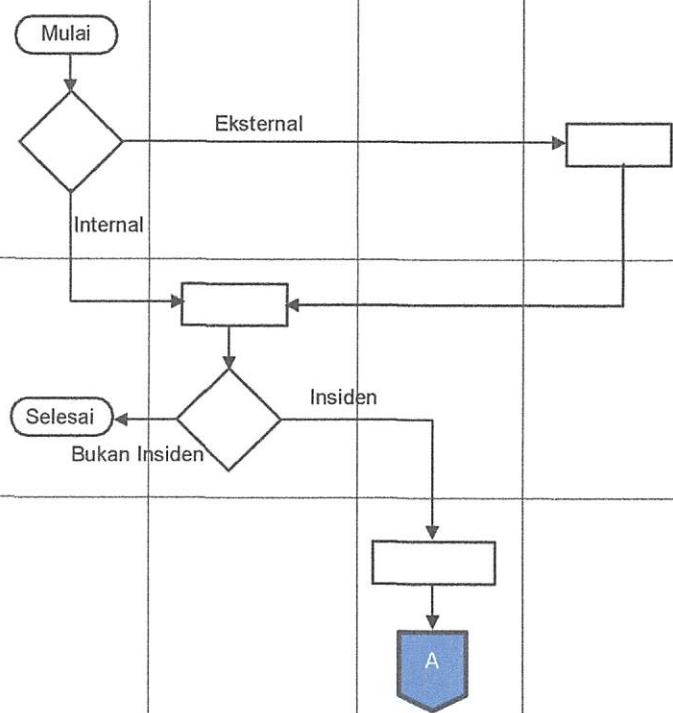
**STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN KEAMANAN INFORMASI PADA PUSAT DATA**

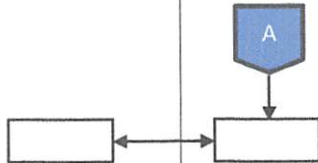
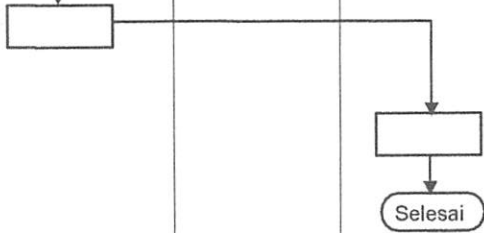
No	Kegiatan	Pelaksana				Mutu Baku		Keterangan
		Pelapor	Bidang Persandian dan Keamanan Informasi	Bidang Layanan E-Government	Ketua CSIRT	Waktu	Output	
1	Menyampaikan laporan/informasi terkait terjadinya insiden keamanan informasi - Jika pelapor eksternal harus membuat surat laporan terjadinya Insiden - Jika Internal tidak	<pre> graph TD Start([Mulai]) --> Dec1{ } Dec1 -- Eksternal --> Box1[] Dec1 -- Internal --> Box2[] </pre>				30 menit	Surat / Laporan	
2	Menerima dan menganalisa laporan/informasi insiden keamanan informasi - Jika termasuk insiden maka dilanjutkan ke proses berikutnya. - Jika bukan insiden maka selesai		<pre> graph TD Box1[] --> Box3[] Box2[] --> Box3 Box3 --> Dec2{ } Dec2 -- Insiden --> Box4[] Dec2 -- Bukan Insiden --> End([Selesai]) </pre>			60 menit	Surat	
3	Melakukan Pemulihan pada Pusat Data			<pre> graph TD Box4[] --> A[A] </pre>		3 HK		

4	Mencatat Hasil Penanganan Insiden Keamanan Informasi pada Pusat Data		 <pre> graph TD A[Shield A] --> B[Process Box] B <--> C[Process Box] </pre>	60 menit	Surat	
5	Melaporkan Hasil Penanganan Insiden Keamanan Informasi pada Pusat Data terdampak		 <pre> graph TD B[Process Box] --> D[Process Box] D --> E[Process Box] E --> F([Selesai]) </pre>	30 menit	Surat	

 PEMERINTAH KOTA CIREBON DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA CIREBON	Nomor SOP	000.8.3.3 / 104 / 2.21 - SANDI / DKIS / 2024
	Tanggal Pembuatan	02 Januari 2024
	Tanggal Revisi	
	Tanggal Efektif	02 Januari 2024
	Disahkan oleh	 Kepala Dinas Komunikasi, Informatika dan Statistik Kota Cirebon  MA'RUF NURYASA, AP.MM. NIP. 19760330 199602 1 004
NAMA SOP : PENANGANAN INSIDEN KEAMANAN INFORMASI PADA JARINGAN		
Dasar Hukum:		Kualifikasi Pelaksana:
1. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; 2. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik; 3. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; 4. Keputusan Wali Kota Cirebon Nomor 048.05/Kep.380 -DKIS/2021 tentang Perubahan atas Keputusan Wali Kota Cirebon Nomor 048.05/Kep.207-DKIS/2021 tentang Pembentukan Tim Tanggap Penanganan Insiden Keamanan Informasi di Pemerintah Daerah Kota Cirebon.		1. Memahami Tugas Pokok dan Fungsi unit kerjanya 2. SDM yang memiliki Kompetensi IT 3. SDM yang memahami peraturan terkait Penanganan Insiden Keamanan Informasi 4. Menguasai SOP Penanganan Insiden Keamanan Informasi
Keterkaitan:		Peralatan / Perlengkapan :
		1. Ruang penanganan insiden 2. Komputer/Laptop 3. Internet
Peringatan:		PENCATATAN DAN PENDAFTARAN:
Apabila SOP ini tidak dilaksanakan dengan baik maka akan menghambat proses Penanganan Insiden Keamanan Informasi pada Pemerintah Daerah Kota Cirebon		Disimpan sebagai data Penanganan Insiden Keamanan Informasi pada Jaringan

**STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN KEAMANAN INFORMASI PADA JARINGAN**

No	Kegiatan	Pelaksana				Mutu Baku		Keterangan
		Pelapor	Bidang Persandian dan Keamanan Informasi	Bidang Infrastruktur dan TIK	Ketua CSIRT	Waktu	Output	
1	Menyampaikan laporan/informasi terkait terjadinya insiden keamanan informasi - Jika pelapor eksternal harus membuat surat laporan terjadinya Insiden - Jika Internal tidak	 <pre> graph TD Start([Mulai]) --> D1{ } D1 -- Eksternal --> R1[] D1 -- Internal --> R2[] R1 --> R2 R2 --> D2{ } D2 -- Insiden --> R3[] D2 -- Bukan Insiden --> End([Selesai]) R3 --> A{{A}} </pre>				30 menit	Surat / Laporan	
2	Menerima dan menganalisa laporan/informasi insiden keamanan informasi - Jika termasuk insiden maka dilanjutkan ke proses berikutnya. - Jika bukan insiden maka selesai					60 menit	Surat	
3	Melakukan Perbaikan Jaringan					120 menit		

4	Mencatat Hasil Penanganan Insiden Keamanan Informasi Jaringan		 <pre>graph TD; A[Icon A] --> B[]; B <--> C[]</pre>	60 menit	Surat	
5	Melaporkan Hasil Penanganan Insiden Keamanan Informasi kepada pemilik/pengelola Jaringan terdampak		 <pre>graph TD; B[] --> D[]; D --> E[]; E --> F([Selesai])</pre>	30 menit	Surat	